What is claimed is:

1. A system for providing Web-based remote security application client administration in a distributed computing environment, comprising:

a self-extracting configuration file containing an executable configuration file that is self-extractable on a target client into an administered security application;

an executable control embedded within an active administration Web page, the executable control being triggered upon each request for the active Web page and causing dynamic Web content to be generated therefrom;

a Web server exporting a Web portal comprising the active administration Web page to a browser application independent of a specific operating environment and interpreting the executable control to facilitate copying of the self-extracting configuration file to the target client.

2. A system according to Claim 1, further comprising:

the Web server facilitating copying of the self-extracting configuration file concurrently to a plurality of target clients.

3. A system according to Claim 1, further comprising:

the Web server checking administrator credentials while exporting the Web portal against a list of authorized administrators.

4. A system according to Claim 1, further comprising:

the Web server monitoring the status of the copying of the self-extracting configuration file to at least one target client.

5. A system according to Claim 1, further comprising:

the Web server reporting the status of security application configuration on at least one target client.

6. A system according to Claim 1, further comprising:

the self-extracting configuration file performing at least one of an installation, configuration, updating, and patching of the security application by executing the executable configuration file.

7. A system according to Claim 1, wherein the executable configuration file comprises at least one of a virus scanning, virus screening, active security, firewall, and VPN performance reporting application.

8. A system according to Claim 1, wherein the executable configuration file is a cabinet archival file.

9. A system according to Claim 1, wherein the active control is an Active X-compliant control.

10. A system according to Claim 1, wherein the distributed computing environment is TCP/IP-compliant.

11. A method for providing Web-based remote security application client administration in a distributed computing environment, comprising:

storing a self-extracting configuration file containing an executable configuration file that is self-extractable on a target client into an administered security application;

providing an executable control embedded within an active administration Web page, the executable control being triggered upon each request for the active Web page and causing dynamic Web content to be generated therefrom;

exporting a Web portal comprising the active administration Web page to a browser application independent of a specific operating environment; and

interpreting the executable control to facilitate copying of the self-extracting configuration file to the target client.

12. A method according to Claim 11, further comprising:

facilitating copying of the self-extracting configuration file concurrently to a plurality of target clients.

13. A method according to Claim 11, further comprising:

checking administrator credentials while exporting the Web portal against a list of authorized administrators.

14. A method according to Claim 11, further comprising:

monitoring the status of the copying of the self-extracting configuration file to at least one target client.

15. A method according to Claim 11, further comprising:

reporting the status of security application configuration on at least one target client.

16. A method according to Claim 11, further comprising:

performing at least one of an installation, configuration, updating, and patching of the security application by executing the executable configuration file.

17. A method according to Claim 11, wherein the executable configuration file comprises at least one of a virus scanning, virus screening, active security, firewall, and VPN performance reporting application.

18. A method according to Claim 11, wherein the executable configuration file is a cabinet archival file.

19. A method according to Claim 11, wherein the active control is an Active X-compliant control.

20. A method according to Claim 11, wherein the distributed computing environment is TCP/IP-compliant.

21. A computer-readable storage medium holding code for performing the method according to Claim 11.

22. A system for remotely administering a client application using a Web-based portal in a TCP/IP-compliant environment, comprising:

an archival configuration file capable of self-extracting on a target client into an executable configuration file;

an executable control into an active administration Web page, the executable control being triggered upon each request for the active Web page and causing dynamic Web content to be generated therefrom;

a Web server serving the active administration Web page to a browser application to a requesting administrator, comprising:

a security module confirming credentials for the requesting administrator against a list of authorized administrators; and

a transfer module interpreting the executable control upon successful credentialing to facilitate substantially concurrent copying of the self-extracting configuration file to at least one target client.

23. A system according to Claim 22, further comprising:

the Web server continuously monitoring the status of the copying of the self-extracting configuration file to the at least one target client; and

the Web server generating a status event upon completion of the copying.

24. A system according to Claim 22, further comprising:

the Web server reporting the status of each application configuration on the at least one target client.

25. A system according to Claim 22, wherein the active control is an Active X-compliant control.

26. A method for remotely administering a client application using a Web-based portal in a TCP/IP-compliant environment, comprising:

storing an archival configuration file capable of self-extracting on a target client into an executable configuration file;

embedding an executable control into an active administration Web page, the executable control being triggered upon each request for the active Web page and causing dynamic Web content to be generated therefrom;

serving the active administration Web page to a browser application to a requesting administrator, comprising:

confirming credentials for the requesting administrator against a list of authorized administrators; and

interpreting the executable control upon successful credentialing to facilitate substantially concurrent copying of the self-extracting configuration file to at least one target client.

27. A method according to Claim 26, further comprising:

continuously monitoring the status of the copying of the self-extracting configuration file to the at least one target client; and

generating a status event upon completion of the copying.

28. A method according to Claim 26, further comprising:

reporting the status of each application configuration on the at least one target client.

29. A method according to Claim 26, wherein the active control is an Active X-compliant control.

30. A computer-readable storage medium holding code for performing the method according to Claim 26.